Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. - 10. (canceled)

11. (new) A certificate validity authentication method for a public key certificate wherein validity of the public key certificate is authenticated by a computer, wherein

the computer executes:

a path search step of searching a path between any one of a plurality of certification authorities as a start point (a start certification authority) and at least one terminal certification authority which issues the public key certificate to terminals;

a path verification step of verifying the path searched by the path searching step;

a path registration step of registering the path verified by the path verification step in a database; and

a validity authentication step of receiving a request to authenticate the public key certificate and validating the public key certificate issued by the terminal certification authorities by using information on the verified path registered in the database, and wherein

the in the path search step, the computer executes:

a first step of setting the start certification authority as an issue origin certification authority;

a second step of obtaining issue destinations of all the public key certificates issued by a device of the issue origin certification authority;

a third step, as to each of the issue destinations obtained in the second step, in a case where the issue destination concerned is one of the plurality of certification authorities, setting a path between the issue destination concerned and the issue origin certification authority, and in a case where the issue destination concerned is one of the terminals, setting the issue origin certification authority as the terminal certification authority, and setting a path comprising at least one of the path thus set, between the start certification authority and the terminal certification authority as the searched path; and

a fourth step, if the issue destinations obtained in the second step include one of the plurality of certification authorities, returning to the second step, and wherein

in the path verification step, the computer executes:

a fifth step of setting the terminal certification authority as the issue destination certification authority;

a sixth step of verifying the signature of the public key certificate issued by the issue destination certification authority with another public key certificate issued by the issue origin certification authority located on the searched path; and

a seventh step, in a case where the signature has been verified and the issue origin certification authority on the searched path is not the start certification authority, setting the issue origin certification authority as a new issue destination certification authority on the searched path and returning to the sixth step, in a case where the signature has been verified and the issue origin certification authority on the searched path is the start certification authority, setting the searched path as a certification path (verified path).

12. (new) A certificate validity authentication method for a public key certificate according to claim 11, wherein

in the validity authentication step, the computer judges that the public key certificate issued by the terminal certification authority is validated if the path between the start certification authority and a certification authority trusted by the authentication request originator and the path between the start certification authority and the terminal certification authority are both contained in the paths registered in the database.

13. (new) Certificate validity authentication method for a public key certificate according to claim 12, wherein

in the validity authentication step, the computer judges that the public key certificate issued by the terminal certification authority is validated if the certification authority trusted by the authentication request originator is the start certification

authority, and the path between the start certification authority and the terminal certification authority is registered in the database.

14. (new) A certificate validity authentication method for a public key certificate according to claim 11, wherein

in the third step, as to each of the issue destinations obtained in the second step, the computer does not set the certification authority as an issue destination certification authority, if the issue destination concerned is the certification authority concerned and the certification authority concerned is included in the paths already set.

15. (new) A certificate validity authentication method for a public key certificate according to claim 11, wherein

the computer executes the path search step independently of the validity authentication step, and executes the path verification step with respect to the path which has been searched and by the path search step, and wherein

in the path registration step, the computer further executes an updating step of updating the registered contents of the database by the path verified by the path verification step.

16. (new) A certificate validity authentication method for a public key certificate according to claim 11, wherein the computer further executes:

a validity term examination step of examining validity term of each of the public key certificates issued by the certificate authorities on each path registered in the database in the registration step;

an obtaining step of attempting to obtain, from the device of the issue origin certification authority of the public key certificate whose validity term has been confirmed to be time-expired in the validity term examination step, a new public key certificate for an issue destination of the public key certificate concerned; and

a path re-verification step of verifying a signature of the newly obtained public key certificate with the public key certificate issued by the device of the certification authority which is the issue destination certification authority of the issue origin certification authority on the path, and wherein

the computer deletes in the path registering step, the path including the public key certificate whose validity term has been confirmed to be time-expired, in either of the case where the validity of the signature of the new public key certificate has not been verified in the path re-verification step or a new public key certification has failed to be obtained in the obtaining step.

17. (new) A certificate validity authentication method for a public key certificate according to claim 11, wherein

the computer further executes an expiration information examination step of examining expiration information of the public key certificate issued by each

certification authority on each of the paths registered in the database in the path registering step, and wherein

the path registration step deletes the path including public key certificate whose validity has been confirmed to be time-expired based on the expiration information obtained in the expiration information examination step.

18. (new) A certificate validity authentication method for a public key certificate according to claim 11, wherein the computer further executes an expiration information examination step of authenticating the public key certificate with the expiration information in the sixth step.

19. (new) A certificate validity authentication method for a public key certificate according to claim 18, wherein

in the expiration information examination step, as to each path registered in the database by the registration step, the computer executes:

an expiration information creation schedule time checking step of checking whether the scheduled time for creating the expiration information for the public key certificate has passed or not for each expiration information of the public key certificate issued by each certification authority;

an obtaining step of obtaining new expiration information on the expiration information whose scheduled time has been confirmed to have passed by the expiration information creation schedule time examination step; and

a term-expired certificate examination step of examining whether the public key certificate given in the newly obtained expiration information is registered in the database or not, wherein

in the path registration step, the computer deletes the path including the term-expired public key certificate which has been confirmed to be time-expired by the term-expired certificate expiration examination step.

20. (new) A certificate validity authentication method for a public key certificate according to claim 11, wherein

in the validity authentication step, the computer judges that the validity of the public key certificate has not been validated, if one of the public key certificates issued by any of the certificate authorities on the path includes a description that the certification authority and a validity authentication request originator is registered in the database.

21. (new) A certificate validity authentication method for a public key certificate according to claim 11, wherein

in the validity authentication step, the computer judges that the public key certificate has not been validated, if a largest possible number of certificate authorities on the path which is written in the public key certificate for the issue destination certification authority on the path issued by any of the certificate authorities on the path, exceeds the total number of the certificate authorities on the

path, even when the path between the start certification authority and the validity authentication request originator is registered in the database.

22. (new) A certificate validity authentication method for a public key certificate according to claim 11, wherein

in the validity authentication step, when the validity authentication request for the public key certificate is accompanied by an indication of reliability degree required for taking electronic procedure, the computer judges that the public key certificate has not been validated, if the reliability degree which is written in the public key certificate for the issue destination certification authority on the path issued by any of the certificate authorities on the path is lower than the reliability required for the electronic procedure, even when the path between the path start certification authority and the validity authentication request originator is registered in the database.

23. (new) A certificate validity authentication method for a public key certificate according to claim 11, wherein

the start certification authority is a bridge certification authority which has cross-certify with each of root certification authorities of at least two security domains.